

MAY 03 2007

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for issuing a digital certificate to a user having an electronic account on a network, comprising the steps of:
 - receiving a request for a digital certificate for the user having the electronic account;
 - sending an identification verification form to a physical address of the user;
 - after the identification verification form is sent, receiving the identification verification form from the user in person at a proofing workstation;
 - after the identification verification form is received, verifying the identity of the user in person using the identification verification form at the proofing workstation;
 - when the identity of the user has been verified, generating the digital certificate by a certificate authority for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network; and
 - linking the digital certificate to the electronic account of the user.
2. (Original) The method of claim 1, further comprising the step of:

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

storing a reference to the digital certificate in a certificate directory at the
certificate authority.

3. (Original) The method of claim 1, wherein the certificate authority includes a proofing server.
4. (Previously Presented) The method of claim 3, wherein the certificate authority further includes the proofing workstation.
5. (Original) The method of claim 1, wherein the certificate authority is a United States Postal Service digital certificate authority.
6. (Original) The method of claim 1, wherein the digital certificate includes an identifier of the user.
7. (Original) The method of claim 1, wherein the digital certificate includes a certificate serial number.
8. (Original) The method of claim 1, wherein the digital certificate includes a certificate validity period.
9. (Original) The method of claim 1, wherein the digital certificate includes a proofing workstation validation.

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

10. (Original) The method of claim 1, wherein the digital certificate includes a public key for authenticating the digital certificate.
11. (Original) The method of claim 1, wherein the digital certificate includes an identifier of the certificate authority.
12. (Original) The method of claim 1, wherein the digital certificate includes a certificate status.
13. (Previously Presented) The method of claim 12, wherein the certificate status is set to active after the identity of the user has been verified in person.
14. (Previously Presented) The method of claim 12, wherein the certificate status is set to hold until the identity of the user is verified in person.
15. (Original) The method of claim 12, wherein the certificate status is set to revoked.
16. (Currently Amended) A method for issuing a digital certificate to a user having an electronic account on a network, comprising the steps of:
 - receiving, at a proofing server, a request for a digital certificate from the user with the electronic account;

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

sending, by the proofing server, an identification verification form to a
physical address of the user;
generating, by the proofing server, the digital certificate for the user;
setting, by the proofing server, a status of the digital certificate to hold;
sending, by the proofing server, the request for the digital certificate to a
proofing workstation;
after the identification verification form is sent, receiving at the proofing
workstation the identification verification form from the user in
person;
after the identification verification form is received, verifying, at the
proofing workstation, the identity of the user via the identification
verification form with information provided by the user in person at
the proofing workstation;
when the identity of the user has been verified, sending by the proofing
workstation an identification verification to the proofing server;
in response to the identification verification, setting, by the proofing server,
the status of the digital certificate to active; and
storing at the proofing server, the digital certificate in the electronic
account of the user.

17. (Original) The method of claim 16, further comprising the step of:

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

linking the digital certificate to a transaction on the network by the user,
wherein the digital certificate can be used to authenticate the
transaction.

18. (Original) The method of claim 16, further comprising the step of:
storing a reference to the digital certificate in a certificate directory at the
proofing server.
19. (Original) The method of claim 16, further comprising the step of:
setting the status of the digital certificate to revoked.
20. (Original) The method of claim 19, further comprising the step of:
storing a reference to the digital certificate in a certificate revocation list at
the proofing server.
21. (Previously Presented) The method of claim 16, further comprising the step of:
sending a private key from the proofing workstation to the proofing server,
when the identity of the user is verified in person.
22. (Original) The method of claim 21, further comprising the step of:
verifying the private key, by the proofing server, before setting the status
of the digital certificate to active.

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

23. (Previously Presented) The method of claim 16, wherein the proofing workstation includes at least one of a bar code scanner, a camera, and a biometric reader.
24. (Previously Presented) The method of claim 23, wherein the identification verification is a bar code read from the identification verification form.
25. (Original) The method of claim 16, wherein the proofing workstation includes a credit card reader.
26. (Previously Presented) The method of claim 16, wherein the proofing workstation includes at least one of a smart card interface, a camera, and a biometric reader.
27. (Original) The method of claim 16, wherein the proofing server is a United States Postal Service proofing server.
28. (Original) The method of claim 16, wherein the proofing workstation is a United States Postal Service proofing workstation.
29. (Currently Amended) A method for processing a request for a digital certificate from a user having an electronic account on a network, comprising the steps of:
receiving, at a proofing workstation, user information for the user with the
electronic account, including an identification verification form
previously sent to a physical address of the user;

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

after receiving the user information, verifying at the proofing workstation,

identification information from the user in person at the proofing

workstation based on the identification verification form;

matching, at the proofing workstation, the user information to the

identification information; and

sending by the proofing workstation to a proofing server, an identification

verification when the user information has been matched to the

identification information received from the user in person.

30. (Original) The method of claim 29, further comprising the step of :
receiving payment from the user at the proofing workstation.
31. (Original) The method of claim 30, wherein the payment is received via credit card.
32. (Previously Presented) The method of claim 30, wherein the payment is received via smart card.
33. (Previously Presented) The method of claim 29, wherein the proofing workstation includes at least one of a bar code reader, a camera, and a biometric reader.
34. (Previously Presented) The method of claim 33, wherein the identification verification is a bar code read from the identification verification form.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

35. (Original) The method of claim 29, wherein the proofing workstation is a United States Postal Service proofing workstation.
36. (Previously Presented) A method for issuing a digital certificate to a user having an electronic account on a network, comprising the steps of:
- receiving, at a proofing server, a request for a digital certificate from the user with the electronic account;
 - sending, by the proofing server, user information to a proofing workstation via the network;
 - generating, by the proofing server, the digital certificate for the user;
 - setting, by the proofing server, a status of the digital certificate to hold;
 - receiving, by the proofing server, an identification verification from the proofing workstation when the identity of the user has been verified in person at the proofing workstation based on an identification verification form previously sent to a physical address of the user;
 - setting by the proofing server the status of the digital certificate to active in response to the in person identification verification; and
 - storing at the proofing workstation, the digital certificate in the electronic account of the user.
37. (Original) The method of claim 36, further comprising the step of:

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

storing a reference to the digital certificate in a certificate directory at the
proofing server.

38. (Original) The method of claim 36, further comprising the step of:

setting the status of the digital certificate to revoked.

39. (Original) The method of claim 38, further comprising the step of:

storing a reference to the digital certificate in a certificate revocation list at
the proofing server.

40. (Previously Presented) The method of claim 36, further comprising the step of:

receiving a private key from the proofing workstation, when the identity of
the user is verified in person.

41. (Original) The method of claim 40, further comprising the step of:

verifying the private key before setting the status of the digital certificate to
active.

42. (Original) The method of claim 36, wherein the proofing server is a United States
Postal Service proofing server.

43. (Currently Amended) A system for issuing a digital certificate to a user having an
electronic account on a network, comprising:

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

a request receiving component configured to receive a request for a digital certificate for a user having an electronic account;
a sending component configured to send an identification verification form to a physical address of the user;
a verifying component configured to receive the identification verification form from the user after the sending component sends the identification verification form and then verify the identity of the user in person at a proofing workstation;
a generating component configured to generate the digital certificate for the user when the identity of the user has been verified in person, wherein the digital certificate includes information enabling authentication of a transaction on the network; and
a linking component configured to link the digital certificate to the electronic account of the user.

44. (Original) The system of claim 43, further comprising:

a storing component configured to store a reference to the digital certificate in a certificate directory at the generating component.

45. (Original) The system of claim 43, wherein the generating component includes a proofing server.

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

46. (Previously Presented) The system of claim 45, wherein the generating component further includes the proofing workstation.
47. (Original) The system of claim 43, wherein the generating component is a United States Postal Service digital certificate authority.
48. (Original) The system of claim 43, wherein the digital certificate includes an identifier of the user.
49. (Original) The system of claim 43, wherein the digital certificate includes a certificate serial number.
50. (Original) The system of claim 43, wherein the digital certificate includes a certificate validity period.
51. (Original) The system of claim 43, wherein the digital certificate includes a proofing workstation validation.
52. (Original) The system of claim 43, wherein the digital certificate includes a public key for authenticating the digital certificate.
53. (Original) The system of claim 43, wherein the digital certificate includes an identifier of the certificate authority.

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

54. (Original) The system of claim 43, wherein the digital certificate includes a certificate status.
55. (Previously Presented) The system of claim 54, wherein the certificate status is set to active after the identity of the user has been verified in person.
56. (Previously Presented) The system of claim 54, wherein the certificate status is set to hold until the identity of the user has been verified in person.
57. (Original) The system of claim 54, wherein the certificate status is set to revoked.
58. (Currently Amended) A system for issuing a digital certificate to a user having an electronic account on a network, comprising:
- a receiving component configured to receive a request for a digital certificate from the user with the electronic account;
 - a sending component configured to send an identification verification form to a physical address of the user;
 - a generating component configured to generate the digital certificate for the user;
 - a hold setting component configured to set a status of the digital certificate to hold, by a proofing server;

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

a request sending component configured to send the request for the digital certificate to a proofing workstation;

a verifying component configured to receive the identification verification from the user in person after the sending component sends the identification verification form and then verify, via the identification verification form, the identity of the user with information provided by the user in person at the proofing workstation;

a verification sending component configured to send an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified in person;

an active setting component configured to set the status of the digital certificate to active in response to the identification verification; and

a storing component configured to store at the proofing server the digital certificate in the electronic account of the user.

59. (Original) The system of claim 58, further comprising:

a linking component configured to link the digital certificate to a transaction on the network by the user, wherein the digital certificate can be used to authenticate the transaction.

60. (Original) The system of claim 58, further comprising:

a reference storing component configured to store a reference to the digital certificate in a certificate directory at the proofing server.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

61. (Original) The system of claim 58, further comprising:
a revoked setting component configured to set the status of the digital
certificate to revoked.
62. (Original) The system of claim 61, further comprising:
a revoked storing component configured to store a reference to the digital
certificate in a certificate revocation list at the proofing server.
63. (Previously Presented) The system of claim 58, further comprising:
a key sending component configured to send a private key from the
proofing workstation to the proofing server, when the identity of the
user is verified in person.
64. (Original) The system of claim 63, further comprising:
a key verifying component configured to verify the private key before
setting the status of the digital certificate to active.
65. (Previously Presented) The system of claim 58, wherein the proofing workstation
includes at least one of a bar code scanner, a camera, and a biometric reader.
66. (Previously Presented) The system of claim 65, wherein the identification
verification is a bar code read from the identification verification form.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

67. (Original) The system of claim 58, wherein the proofing workstation includes a credit card reader.
68. (Previously Presented) The system of claim 58, wherein the proofing workstation includes at least one of a smart card interface, a camera, and a biometric reader.
69. (Original) The system of claim 58, wherein the proofing server is a United States Postal Service proofing server.
70. (Original) The system of claim 58, wherein the proofing workstation is a United States Postal Service proofing workstation.
71. (Currently Amended) A system for processing a request for a digital certificate from a user having an electronic account on a network, comprising:
- a user information receiving component configured to receive user information for the user with the electronic account including an identification verification form previously sent to a physical address of the user;
 - a verifying component configured to verify identification information from the user in person at a proofing workstation based on the identification verification form after the user information receiving component receives the user information;

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

a matching component configured to match at the proofing workstation the user information to the identification information; and
a verification sending component configured to send, via the identification verification form, an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information received from the user in person.

72. (Original) The system of claim 71, further comprising:
a payment receiving component configured to receive payment from the user at the proofing workstation.
73. (Original) The system of claim 72, wherein the payment is received via credit card.
74. (Previously Presented) The system of claim 72, wherein the payment is received via smart card.
75. (Previously Presented) The system of claim 71, wherein the proofing workstation includes at least one of a bar code reader, a camera, and a biometric reader.
76. (Previously Presented) The system of claim 75, wherein the identification verification is a bar code read from the identification verification form.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

77. (Original) The system of claim 71, wherein the proofing workstation is a United States Postal Service proofing workstation.
78. (Previously Presented) A system for issuing a digital certificate to a user having an electronic account on a network, comprising:
- a request receiving component configured to receive, at a proofing server, a request for a digital certificate from the user with the electronic account;
 - a user information sending component configured to send by the proofing server user information to a proofing workstation via the network;
 - a certificate generating component configured to generate the digital certificate for the user;
 - a hold setting component configured to set, by the proofing server, a status of the digital certificate to hold;
 - a verification receiving component configured to receive, by the proofing server, an identification verification from the proofing workstation when the identity of the user has been verified in person at the proofing workstation based on an identification verification form previously sent to a physical address of the user;
 - an active setting component configured to set by the proofing server the status of the digital certificate to active in response to the in person identification verification; and

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

a storing component configured to store at the proofing server the digital certificate in the electronic account of the user.

79. (Original) The system of claim 78, further comprising:

a reference storing component configured to store a reference to the digital certificate in a certificate directory at the proofing server.

80. (Original) The system of claim 78, further comprising:

a revoked setting component configured to set the status of the digital certificate to revoked.

81. (Original) The system of claim 80, further comprising:

a revoked storing component configured to store a reference to the digital certificate in a certificate revocation list at the proofing server.

82. (Previously Presented) The system of claim 78, further comprising:

a key receiving component configured to receive a private key from the proofing workstation, when the identity of the user is verified in person.

83. (Original) The system of claim 82, further comprising:

a key verifying component configured to verify the private key before setting the status of the digital certificate to active.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

84. (Original) The system of claim 78, wherein the proofing server is a United States Postal Service proofing server.
85. (Currently Amended) A computer readable medium having computer readable code embodied therein for issuing a digital certificate to a user having an electronic account on a network, the computer readable code comprising:
- a request receiving module configured to receive a request for a digital certificate for the user having the electronic account;
 - a sending module configured to send an identification verification form to a physical address of the user;
 - a verifying module configured to receive the identification verification form from the user after the sending module sends the identification verification form and then verify the identity of the user in person at a proofing workstation;
 - a generating module configured to generate the digital certificate for the user when the identity of the user has been verified in person, wherein the digital certificate includes information enabling authentication of a transaction on the network; and
 - a linking module configured to link the digital certificate to the electronic account of the user.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

86. (Currently Amended) A computer readable medium having computer readable code embodied therein for issuing a digital certificate to a user having an electronic account on a network, the computer readable code comprising:
- a request receiving module configured to receive a request for a digital certificate from the user with the electronic account;
 - a sending module configured to send an identification verification form to a physical address of the user;
 - a generating module configured to generate the digital certificate for the user;
 - a hold setting module configured to set a status of the digital certificate to hold, by a proofing server;
 - a request sending module configured to send the request for the digital certificate to a proofing workstation;
 - an identity verifying module configured to receive the identification verification form from the user in person after the sending module sends the identification verification and then verify, via the identification verification form, the identity of the user with information provided by the user in person at the proofing workstation;
 - a verification sending module configured to send an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified in person;

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

an active setting module configured to set the status of the digital
certificate to active in response to the identification verification; and
a storing module configured to store at the proofing server the digital
certificate in the electronic account of the user.

87. (Previously Presented) A computer readable medium having computer readable code embodied therein for processing a request for a digital certificate from a user having an electronic account on a network, the computer readable code comprising:

an information receiving module configured to receive user information for the user with the electronic account;
a verifying module configured to verify identification information from the user in person at a proofing workstation based on an identification verification form previously sent to a physical address of the user;
a matching module configured to match at the proofing workstation the user information to the identification information; and
a sending module configured to send, via the identification verification form, an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information received from the user in person.

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

88. (Previously Presented) A computer readable medium having computer readable code embodied therein for issuing a digital certificate to a user having an electronic account on a network, the computer readable code comprising:

a request receiving module configured to receive, at a proofing server, a request for a digital certificate from the user with the electronic account;

a user information sending module configured to send by the proofing server user information to a proofing workstation via the network;

a generating module configured to generate the digital certificate for the user;

a hold setting module configured to set, by the proofing server, a status of the digital certificate to hold;

a verification receiving module configured to receive, by the proofing server, an identification verification from a proofing workstation when the identity of the user has been verified in person at the proofing workstation based on an identification verification form previously sent to a physical address of the user;

an active setting module configured to set by the proofing server the status of the digital certificate to active in response to the in person identification verification; and

a storing module configured to store at the proofing server the digital certificate in the electronic account of the user.

Attorney Docket No. 08049.0002-00000
Application No. 09/809,325

89. (Currently Amended) A system for issuing a digital certificate to a user having an electronic account on a network, comprising:

means for receiving a request for a digital certificate for the user having the electronic account;

means for sending an identification verification form to a physical address of the user;

means for receiving the identification verification form from the user in person at a proofing workstation after the identification verification form is sent and then verifying the identity of the user in person using the identification verification form at the proofing workstation;

means for generating, by a certificate authority, the digital certificate for the user when the identity of the user has been verified in person, wherein the digital certificate includes information enabling authentication of a transaction on the network; and

means for linking the digital certificate to the electronic account of the user.

90. (Currently Amended) A system for issuing a digital certificate to a user having an electronic account on a network, comprising:

means for receiving, at a proofing server, a request for a digital certificate from the user with the electronic account;

means for sending an identification verification form to a physical address of the user;

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

means for generating, by the proofing server, the digital certificate for the user;

means for setting, by the proofing server, a status of the digital certificate to hold, by the proofing server;

means for sending, by the proofing server, the request for the digital certificate to a proofing workstation;

means for receiving the identification verification form from the user in person at the proofing workstation after the identification verification form is sent;

means for verifying, via the identification verification form at the proofing workstation, the identity of the user with information provided by the user in person at the proofing workstation after the identification verification form is received;

means for sending an identification verification from the proofing workstation to the proofing server, when the identity of the user is verified;

means for setting, by the proofing server, the status of the digital certificate to active in response to the identification verification; and

means for storing at the proofing server the digital certificate in the electronic account of the user.

91. (Currently Amended) A system for processing a request for a digital certificate from a user having an electronic account on a network, comprising:

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

means for receiving, at a proofing workstation, user information for the user with the electronic account, including an identification verification form previously sent to a physical address of the user;

means for verifying at the proofing workstation identification information from the user in person at the proofing workstation based on the identification verification form after the user information is received;

means for matching, at the proofing workstation, the user information to the identification information; and

means for sending, via the identification verification form, an identification verification from the proofing workstation to a proofing server, when the user information has been matched to the identification information received from the user in person.

92. (Previously Presented) A system for issuing a digital certificate to a user having an electronic account on a network, comprising:

means for receiving, at a proofing server, a request for a digital certificate from the user with the electronic account;

means for sending by the proofing server user information to a proofing workstation via the network;

means for generating, by the proofing server, the digital certificate for the user;

means for setting, by the proofing server, a status of the digital certificate to hold;

Attorney Docket No. 08049.0002-00000

Application No. 09/809,325

means for receiving, by the proofing server, an identification verification from the proofing workstation when the identity of the user has been verified in person at the proofing workstation based on an identification verification form previously sent to a physical address of the user;

means for setting, by the proofing server, the status of the digital certificate to active in response to the in person identification verification; and

means for storing at the proofing workstation the digital certificate in the electronic account of the user.